

Physical Equivalence of Pure States and Derivation of Qubit in General Probabilistic Theories

Gen Kimura ^{[a],[*]}, Koji Nuida ^{[b],†} and Hideki Imai ^{[b],[c]}

^[a] *Research and Development Initiative, Chuo University,
1-13-27 Kasuga, Bunkyo-ku, Tokyo 112-8551, Japan and*

^[b] *Research Center for Information Security (RCIS),
National Institute of Advanced Industrial Science and Technology (AIST). Daibiru building 1003,
1-18-13 Sotokanda, Chiyoda-ku, Tokyo, 101-0021, Japan*

^[c] *Graduate School of Science and Engineering,
Chuo University. 1-13-27 Kasuga, Bunkyo-ku, Tokyo 112-8551, Japan*

In this paper, we investigate a characterization of Quantum Mechanics by two physical principles based on general probabilistic theories. We first give the operationally motivated definition of the physical equivalence of states and consider the principle of the physical equivalence of pure states, which turns out to be equivalent to the symmetric structure of the state space. We further consider another principle of the decomposability with distinguishable pure states. We give classification theorems of the state spaces for each principle, and derive the Bloch ball in 2 and 3 dimensional systems by these principles.

I. INTRODUCTION

After the completion of von Neumann’s celebrated axioms [1] of Quantum Mechanics (QM), one of the theoretical and philosophical interests of QM shifted to derive the theory using solely physical principles. Here the physical principle means a physical statement which is, in principle, testable by experiments. For instance, a statement such as “a quantum observable is represented by a self-adjoint operator on a Hilbert space” is not a physical principle, but a statement such as “the speed of light is constant independent of observer’s motion” gives a typical example of a physical principle. Indeed, the standard axioms of QM presuppose a priori mathematical structures such as Hilbert space and linear operators — as the former example is one of the axioms — and then gives a recipe (Born’s rule) of how to predict physical phenomena by combining such mathematical objects. This non-physical characterization of QM is sometimes considered as one of the causes why QM is difficult to intuitively understand — in the end, many students who learn QM for the first time naively ask themselves “Why observables are described by (non-commutative) operators?” On the other hand, if QM was constructed solely with physical principles and if, moreover, they are tested by experiments, then QM would be intuitively more acceptable than the present situation, as all the “weird” quantum phenomena (such as the uncertainty principle and an entanglement) automatically follow from experimentally established phenomena. (For instance, most physicists feel to intuitively understand the relativity of time, even though contrary to our common sense, since they know that the invariance of the speed of light is ex-

perimentally confirmed and the fact naturally leads the relativity of time.)

Therefore, a desire to derive axioms of QM which are purely described by physical principles is natural as many researchers indeed have tackled this problem so far [2–7], and some of recent developments in [8–10] and [11] contribute the goal in each ways.

One of the lines of this research starts by recognizing that QM is one of the probabilistic theories. Indeed, with the standard interpretation of QM and indeed with a practical method to compare with experimental data, what QM predicts is a probability to obtain an outcome by performing a measurement under a given state. However, the structure of the theory is more complicated than a classical probability theory (based on Kolmogorov’s axioms). Therefore, it is convenient to first establish a general framework for all the possible probabilistic models including both classical theory and QM. Then, we can look for particular conditions (described by physical principles) which narrow down the general models to be QM. Indeed, such a general framework has been well investigated (for instance see [12–16]) and recently is called General Probabilistic Theories (GPTs) [17–19].

For this purpose, we first give an operationally motivated definition of the physical equivalence between states and propose a physical principle of [P5] *Physical Equivalence of Pure States*. Then we show that the principle is equivalently described by a symmetric structure of state space (See Theorem 2 and the principle [P5’]). Next, we consider another principle of [P6] the decomposability with distinguishable pure states. We give representation theorems for state spaces for each principle (See Proposition 5, Theorems 5, 6 for [P5], and Theorem 7 for [P6]). By combining these results, we derive that GPTs with 2 or 3 dimensional state spaces are either classical or quantum (See Theorem 8). Our results are closely related to those in [8–10] and [11], where the general Bloch ball is obtained. However, the definition of the Bloch ball there is given by a system with at

*Electronic address: gen-kimura[at]aist.go.jp

†Electronic address: k.nuida[at]aist.go.jp

most two distinguishable states. On the other hand, we do not require the maximum number of distinguishable states and discuss how the state space is characterized. To understand this non-triviality, we notice that a state space is not uniquely determined under the above two principles but on the contrary still there admits a complicated state space, where the typical example is given by QM itself with more than or equal to 3 dimensional Hilbert spaces (see [20]). Notice that in this paper we do not deal with a dynamics, a measurement process, nor a composite system, which are another important notions for GPTs. Rather, we are interested in how GPTs are characterized with the above minimum restrictions (principles) posed only on states and measurements.

This paper is organized as follows. In Sec. II, we review and reconstruct GPTs with natural physical principles [P1-P3], especially explaining the basic notions of states and measurements and how mathematical structures such as vectors in a real vector space appear to represent them. In Sec. III, we introduce and investigate the principles [P5] and [P6], including general discussion of the invariant states under any affine bijection on the state space. In Sec. IV, we give a concluding remark and discussion.

II. REVIEW OF GENERAL PROBABILISTIC THEORIES

In this section, we briefly review General Probabilistic Theories (GPTs) as a general framework of operationally well-defined probabilistic models, focusing on the notions of states and measurements. Based on operationally motivated principles, we explain how states and measurements are mathematically represented by vectors in a compact convex set and effects, respectively. It is important to recognize that these mathematical structures are not introduced a priori but they are the consequences from physical principles.

A. States and Measurements on GPTs

The basic ingredients of GPTs are the notions of *states* and *measurements* with a physical law (e.g., Born's Rule in quantum mechanics) to predict a probability to obtain a measurement outcome. Formally, we assume the following:

[P1] (Probability Assignment Principle) *A probability $\Pr\{M = m_i|s\}$ to get an outcome m_i is given when performing a measurement M under a state s :*

$$\Pr\{M = m_i|s\} \geq 0, \sum_{i=1}^n \Pr\{M = m_i|s\} = 1. \quad (1)$$

In this paper, we assume for mathematical simplicity that each measurement M has a discrete (and finite) set of measurement outcomes $\{m_i\}_{i=1}^n$ with $n \geq 1$ [38].

In particular, 2-valued measurements with $n = 2$ (Yes-No measurements) play a fundamental role as building blocks of any measurements (See for instance Chapter 6 in [21]). In the following, the symbols s, s_1, s_2, \dots , M, M_1, M_2, \dots and m, m_1, m_2, \dots represent states, measurements and measurement outcomes, respectively.

With an operational view, we naturally identify states s_1 and s_2 if there are no physical differences between them. In our case, the only method to compare physical properties of states is to observe probabilities given through possible measurements. Thus we may assume the following:

[P2-1] (Separation Principles for States) *States s_1 and s_2 are identified iff $\Pr\{M = m_i|s_1\} = \Pr\{M = m_i|s_2\}$ for any measurement M and measurement outcome m_i .*

Indeed, the preliminary notion of “state” in an operational view is defined by a preparation of experimental instruments (settings). Then, a state is defined by the equivalence class among all the “states” having the same physical properties, which in our case are the probability distributions among possible measurements. Therefore, one may interpret [P2-1] as one aspect of a natural definition of states.

The similar argument follows for measurements. Namely, we identify measurements if there are no physical differences among them under any states. It is also convenient to drop the information of measurement outcome m_i by identifying them just as an i th outcome. By doing so, we denote by $\Pr\{M = i|s\} := \Pr\{M = m_i|s\}$ the probability to get i th outcome when performing a measurement M under a state s . Thus we identify n -valued measurements M and M' irrespective of the set of outcome if their statistical properties are identical for each outcome. Therefore, we assume the following:

[P2-2] (Separation Principles for Measurements) *Measurements M_1 and M_2 with the same number of outcomes are identified iff $\Pr\{M_1 = i|s\} = \Pr\{M_2 = i|s\}$ for any i and state s .*

It is operationally natural to allow a probabilistic mixture of states as one of the procedures to prepare states. Namely, if states s_1 and s_2 can be prepared, a preparation of state s_1 with probability p and state s_2 with probability $1-p$ can also be prepared. With this preparation, the probability for any measurement should satisfy the mixing property due to the union rule of the probability and the definition of the conditional probability. Formally, we thus assume the following:

[P3-1] (Mixing Principle for States) *For any state s_1, s_2 and for any $p \in [0, 1]$, there exists a state s satisfying $\Pr\{M = i|s\} = p\Pr\{M = i|s_1\} + (1-p)\Pr\{M = i|s_2\}$ for any measurement M and i .*

Of course, we implicitly suppose that the above state s can be prepared as a probabilistic mixture of s_1 and s_2 with probabilities p and $1-p$. From [P2-1], it is uniquely determined with given s_1, s_2 and p , and is denoted by $s = \langle p; s_1, s_2 \rangle$ [14]. Note that the trivial mixtures $s = \langle p; s, s \rangle$ and $s = \langle 1; s, s' \rangle = \langle 0; s', s \rangle$ follow for any state s, s' and $p \in [0, 1]$. A state is called a *pure* state iff there exist no

means to prepare it with nontrivial probabilistic mixture. Namely, s is a pure state iff $s = \langle p; s_1, s_2 \rangle$ for states s_1, s_2 and $p \in (0, 1)$ implies $s_1 = s_2$. Otherwise, a state is called a *mixed* state. In the following, we denote the set of all states and pure states by \mathcal{S} and $\mathcal{S}_{\text{pure}}$, respectively. \mathcal{S} is called the *state space*.

Similarly, it is operationally legitimate to allow a probabilistic mixture of measurements: Namely, if n -valued measurements M_1 and M_2 can be performed, then a measurement to perform M_1 with probability p and M_2 with probability $1 - p$ is also possible:

[P3-2] (Mixing Principle for Measurements) *For any n -valued measurement M_1, M_2 , and for any $p \in [0, 1]$ there exists an n -valued measurement M satisfying $\Pr\{M = i|s\} = p\Pr\{M_1 = i|s\} + (1 - p)\Pr\{M_2 = i|s\}$ for any $i = 1, \dots, n$ and state s .*

From [P2-2], the measurement M with given M_1, M_2, p in [P3-2] is uniquely determined up to arbitrary choice of measurement outcomes.

So far, we have only assumed natural principles [P1]-[P3] resorting to no *a priori* mathematical structures. However, it turns out that states and measurements are represented by vectors in a real vector space as follows:

[Representation 1] (i) *A state is represented by a vector in a real vector space V such that a convex combination of states s_1 and s_2 with weight p represents the state $\langle p; s_1, s_2 \rangle$; Thus the state space \mathcal{S} is a convex subset of V and pure states correspond to extreme points of \mathcal{S} .* (ii) *An n -valued measurement M is represented by an n -tuple of effects $(e_i)_{i=1}^n$ on \mathcal{S} such that $\sum_i e_i = u$, meaning that $e_i(s)$ is the probability to get i th outcome when performing the measurement M under a state s .*

Remind the following mathematical terminologies: a subset W in a real vector space is called a convex subset iff it is closed under any convex combinations. A vector $w \in W$ is called an extreme point iff w has no non-trivial convex decompositions in W , i.e., $w = pw_1 + (1 - p)w_2$ for some $w_1, w_2 \in W$ and $p \in (0, 1)$ implies $w = w_1 = w_2$. A real functional $f : W \rightarrow \mathbb{R}$ is called an affine functional on W iff $f(pw_1 + (1 - p)w_2) = pf(w_1) + (1 - p)f(w_2)$ for any $w_1, w_2 \in W$ and $p \in [0, 1]$. An affine functional e on W is called an *effect* on W iff the range is in $[0, 1]$. The unit effect and the zero effect, denoted by u and 0 , are effects defined by $u(s) = 1, 0(s) = 0$ for all $s \in W$. For the readers' convenience, we present the precise proof of Representation 1 in Appendix A (See Theorem 9).

Notice that a representation of states and measurements is of course not unique. GPTs with state representations $\mathcal{S} \subset V$ and $\mathcal{S}' \subset V'$ in real vector spaces V, V' are equivalent (hereafter *affine isomorphic*) iff there exists an affine bijection $\Lambda : \mathcal{S} \rightarrow \mathcal{S}'$ such that the correspondent of measurement $M = (e_i)_{i=1}^n$ on \mathcal{S} is given by $M' = (e_i \circ \Lambda^{-1})_{i=1}^n$ on \mathcal{S}' . In particular, if the (affine) dimension of \mathcal{S} is finite, one may represent states as vectors in an Euclidean space.

In the following, we use the Representation 1 and let \mathcal{S} be a state space of a vector representation as above. We denote by $\mathcal{A}(\mathcal{S})$ and $\mathcal{E}(\mathcal{S})$ (or simply \mathcal{A} and \mathcal{E}) the

sets of all the affine functionals and effects on \mathcal{S} . It is easy to show that $\mathcal{A}(\mathcal{S})$ is a real vector space with point-wise sum and multiplication and $\mathcal{E}(\mathcal{S})$ is a convex subset of $\mathcal{A}(\mathcal{S})$. An extreme point of $\mathcal{E}(\mathcal{S})$ is called a decision effect (or a pure effect) [4, 19].

Notice that, while any measurement M is represented by an n -tuples $(e_i)_{i=1}^n$ of effects on \mathcal{S} satisfying $\sum_i e_i = u$, the opposite might not hold in general. However, as it is satisfied in both classical and quantum systems (see Sec. IIB), in this paper we assume the following postulate:

[P4] *Given a state space \mathcal{S} , any mathematically well-defined measurement on \mathcal{S} is feasible. Namely, for any n -tuples of effects $(e_i)_{i=1}^n$ with $\sum_i e_i = u$, there exists the corresponding measurement M such that M is represented by $(e_i)_i$.*

With this condition, it turns out that only one has to specify is the state space of GPT, since then feasible measurements are automatically given by effects on \mathcal{S} .

In this paper, we assume [P1-P4] as basic principles for operationally well-defined probabilistic models.

Next, we explain that a natural topology is introduced into a state space. Note that any physical measurements are accompanied by a finite (even small) error. Thus, it is operationally natural to say that states s_1 and s_2 are close iff for arbitrary but finite numbers of measurements the probabilities by measuring them under s_1 and s_2 are within an arbitrary small error. This defines the so-called *physical topology* [13]. With this natural topology, we can go further from the Representation 1:

[Representation 2] *A state is represented by a vector in a locally convex Hausdorff topological vector space V such that the topology is given by the physical topology and — without loss of generality — the state space is a compact convex subset of V . In particular, if $\dim(\mathcal{S}) =: d < \infty$, a state is represented by a vector in \mathbb{R}^d such that the physical topology is the Euclidean topology and \mathcal{S} is a compact (i.e., closed and bounded) convex subset in \mathbb{R}^d .*

Note that $\dim \mathcal{S}$ is the dimension of the affine hull $\text{Aff}(\mathcal{S}) := \{\sum_i \lambda_i s_i \mid w_i \in \mathcal{S}, \lambda_i \in \mathbb{R}, \sum_i \lambda_i = 1\}$. We refer [22] for a (locally convex Hausdorff) topological vector space V . Remind that if V is finite dimensional, then the topology is unique. Thus, if $V = \mathbb{R}^d$, then the unique topology is given by the Euclidean topology of \mathbb{R}^d . Any non-empty compact convex subset W of V has the non-empty set of extreme points of W and is the closed convex hull of extreme points (Krein-Milman Theorem). In finite dimensional case, any vector $w \in W$ has a convex decomposition with finite numbers of extreme points: $w = \sum_{i=1}^m p_i w_i$ with extreme points $\{w_i\}_i$ and a probability distribution $(p_i)_{i=1}^m$ (see, for instance, Theorem 5.6 in [23]). Therefore, in any GPTs, there exist enough pure states so that \mathcal{S} is a closed convex hull of $\mathcal{S}_{\text{pure}}$. Physically speaking, any state s is approximately (in the sense of the physical topology) prepared with a probabilistic mixture of finite numbers of pure states. If $\dim \text{Aff}(\mathcal{S}) < \infty$, any state s is exactly prepared with a probabilistic mixture of finite numbers of pure states

(hereafter, a pure-state decomposition). For the readers' convenience, Representation 2 is explained in details in the case of finite dimension in Appendix B. Indeed, one can introduce a natural norm on V and all the topological issues can be described with this norm in the finite dimensional case. (See [13] and [18] for infinite dimensional cases.)

In the following, we restrict ourselves to finite dimensional GPTs where the state space \mathcal{S} is embedded into a finite dimensional vector space V . For the underlying vector space, we assume without loss of generality $V := \text{Aff}(\mathcal{S})$. In particular, one can assume \mathcal{S} to be a compact (i.e., closed and bounded) convex subset in a Euclidean space \mathbb{R}^d noting that the Euclidean topology coincides with the physical topology.

Notice that, for any state s , one can define an affine functional $\Lambda_s : \mathcal{E} \rightarrow [0, 1]$ by

$$\Lambda_s(e) := e(s) \quad (\forall e \in \mathcal{E}),$$

which satisfies $\Lambda_s(u) = 1$ and $\Lambda_s(0) = 0$. From [P2-1], we have $\Lambda_{s_1} = \Lambda_{s_2}$ iff $s_1 = s_2$. Therefore, a state is represented by an affine functional $\Lambda : \mathcal{E} \rightarrow [0, 1]$ satisfying $\Lambda(u) = 1$ and $\Lambda(0) = 0$. (Indeed, in Appendix A, a vector representation of states is introduced in this way.) It is interesting to notice that the converse is also true:

Theorem 1 *Let Λ be an affine functional on $\mathcal{E} = \mathcal{E}(\mathcal{S})$ such that $\Lambda(e) \in [0, 1]$ for any $e \in \mathcal{E}$ and $\Lambda(u) = 1, \Lambda(0) = 0$. Then, there exists the unique state $s \in \mathcal{S}$ such that $\Lambda(e) = e(s)$ for any $e \in \mathcal{E}$.*

(The proof of this theorem is given in Appendix D.) Therefore, one can identify states and affine functionals on \mathcal{E} satisfying the above properties. In the following, we omit the symbol Λ_s and just write

$$s(e) = e(s), \quad (2)$$

meaning that $s(e) := \Lambda_s(e)$.

To complete the framework of GPTs, one still needs another important notions of transformation (dynamics), measurement process [24], and especially composition of systems. In this paper, we consider GPTs only from the viewpoints of states and measurements by considering how physical principles posed only on states and measurements can narrow down GPTs. This means, of course, that there remains a freedom to further specify GPTs by using another principles on dynamics, composition of systems, etc. [8–10].

B. Examples of GPTs

The typical examples of GPTs are Classical Probability Theory and QM. Here, we briefly review the finite cases for classical theory and QM:

[Example 1] (Finite Classical Probability Theory) A state of a finite classical probability theory is described by a probability distribution $\mathbf{p} = (p_1, \dots, p_c)$ on a sample

space $\Omega_c = \{\omega_1, \omega_2, \dots, \omega_c\}$, and the state space is given by $\mathcal{S}_{cl} := \{\mathbf{p} = (p_1, \dots, p_c) \mid p_i \geq 0, \sum_i p_i = 1\} \subset \mathbb{R}^c$. There exist c numbers of pure states (vertices): $\mathbf{p}^{(1)} = (1, 0, \dots, 0), \dots, \mathbf{p}^{(c)} = (0, \dots, 0, 1)$. Geometrically \mathcal{S}_{cl} is the $c - 1$ dimensional (standard) simplex. [39].

Any classical state $\mathbf{p} = (p_1, \dots, p_c) \in \mathcal{S}_{cl}$ has the unique decomposition into pure states: $\mathbf{p} = \sum_{j=1}^c p_j \mathbf{p}^{(j)}$, and it is convenient to represent an effect e by c dimensional vector $(x_1, \dots, x_c) \in [0, 1]^c$ by $x_i := e(\mathbf{p}^{(i)})$ with $e(\mathbf{p}) = \sum_j p_j x_j$. We write $e \simeq (x_1, \dots, x_c)$ in this case. Note that $u \simeq (1, \dots, 1)$ and $0 \simeq (0, \dots, 0)$. It is easy to see that $\mathcal{E}(\mathcal{S}_{cl}) =: \mathcal{E}_{cl} \simeq [0, 1]^c$, so there are 2^c decision effects (i.e., extreme points of \mathcal{E}_{cl}): $e^{i_1 i_2 \dots i_c} \simeq (i_1, i_2, \dots, i_c)$ where $i_1, \dots, i_c = 0, 1$. Any measurement $M = (e_i)_{i=1}^n$ is represented by n vectors $e_i \simeq (x_1^{(i)}, \dots, x_c^{(i)}) \in [0, 1]^c$ such that $\sum_j x_j^{(i)} = 1$. Typical measurement is given by that of random variable $f : \Omega_c \rightarrow \{m_1, \dots, m_n\}$ where $\Pr\{f = m_i | \mathbf{p}\} := \sum_{j: m_i = f(j)} p_j = \sum_{i=1}^c \delta_{m_i f(j)} p_j$. Since $(\delta_{m_i f(j)})_{j=1}^c$ is one of decision effects, a measurement of random variable corresponds to a measurement with respect to decision effects.

Note that any c -simplex is affine isomorphic to the c -dimensional standard simplex. Therefore, any GPT with simplex-state space is a classical system.

[Example 2] (Finite Quantum Mechanics) A state of a finite QM is represented by a density operator ρ (a positive operator with unit trace, denoted as $\rho \geq 0$ and $\text{tr} \rho = 1$) on a c dimensional Hilbert space \mathcal{H}_c . The state space is thus given by $\mathcal{S}_q := \{\rho \in \mathcal{L}(\mathcal{H}_c) \mid \rho \geq 0, \text{tr} \rho = 1\} \subset \mathcal{L}(\mathcal{H}_c)_h$, where $\mathcal{L}(\mathcal{H}_c)$ ($\mathcal{L}(\mathcal{H}_c)_h$) is the set of all the linear (Hermitian) operators on \mathcal{H}_c . Pure states correspond to the one dimensional projection operators, i.e., $\rho = |\psi\rangle\langle\psi|$ with unit vector $\psi \in \mathcal{H}_c$. A quantum effect e is usually represented by a positive operator $E \in \mathcal{L}(\mathcal{H}_c)$ such that $e(\rho) = \text{tr}(E\rho)$ given by $E := \sum_{i,j=1}^c \tilde{e}(|\psi_i\rangle\langle\psi_j|)|\psi_j\rangle\langle\psi_i|$ with an arbitrary orthonormal basis $\{|\psi_i\rangle\}_{i=1}^c$ of \mathcal{H}_c , where \tilde{e} is a linear extension of e to $\mathcal{L}(\mathcal{H}_c)$ (See Appendix C). Note that the unit and zero effects $u, 0$ correspond to the unit and zero operators \mathbb{I} and 0 , respectively. It is easy to see that $\mathcal{E}_q := \mathcal{E}(\mathcal{S}_q) \simeq \mathcal{L}(\mathcal{H}_c)_{povm} := \{E \in \mathcal{L}(\mathcal{H}_c) \mid 0 \leq E \leq \mathbb{I}\}$, the element of which is called a POVM (positive operator valued measure) element. Thus, any measurement $M = (e_i)_{i=1}^n$ is represented by n -tuple of POVM elements $e_i \simeq E_i \in \mathcal{L}(\mathcal{H}_c)_{povm}$ such that $\sum_{i=1}^n E_i = \mathbb{I}$, which is called a (discrete) POVM. The decision effects correspond to projection operators.

The most elementary quantum system is a qubit system with 2 dimensional Hilbert space \mathcal{H}_2 . For a qubit system, the Bloch vector $\mathbf{b} = (b_1, b_2, b_3) \in \mathbb{R}^3$, defined by $\mathcal{S}_q \ni \rho \mapsto \mathbf{b}_i = \text{tr}(\sigma_i \rho)$ ($i = 1, 2, 3$), gives a useful state representation. (Here, σ_i ($i = 1, 2, 3$) are Pauli spin matrices). Remind that the state space is then given by a unit ball $B := \{\mathbf{b} \in \mathbb{R}^3 \mid \sum_i b_i^2 = 1\} \subset \mathbb{R}^3$ [25].

Notice again that both classical and quantum theories satisfy [P4], i.e., any mathematically well-defined mea-

surement corresponds to a feasible measurement by admitting the so-called indirect measurement [40].

III. ADDITIONAL PRINCIPLES

In the previous section, GPTs are explained as operationally well-defined probability models based on natural principles [P1]-[P4]. In this section, we further consider additional two principles of [P5] *physical equivalence of pure states* and [P6] *decomposability with distinguishable pure states*.

A. Physical Equivalence of Pure States

Intuitively, it seems natural to assume that all the pure states are physically equivalent, i.e., there are no physically exceptional pure states in nature due to its symmetry. This would be acceptable if one reminds both classical and quantum cases, where in both cases there are no structural differences in the set of pure states. (For instance, consider a one dimensional classical particle, where the set of pure states is the phase space \mathbb{R}^2 of the position and the momentum. Obviously, there are no exceptional points in \mathbb{R}^2 . Also in quantum systems, there are no exceptional vectors (pure states) in Hilbert space.) As this argument yet resorts to a rough intuition, we consider here what we exactly mean by the physical equivalence of states with an operational view point of measurements.

First of all, we would like to express that states $s_1, s_2 \in \mathcal{S}$ are physically equivalent if there are no different physical structures on s_1 and s_2 through measurements. This would be naturally characterized by saying the following: For any measurement $E = (e_i)_{i=1}^n$, there uniquely exists the corresponding measurement $F = (f_i)_{i=1}^n$ such that the probability distributions on s_1 by E and s_2 by F are the same: $e_i(s_1) = f_i(s_2)$; Next, this correspondence of the measurements should preserve the affine structures for a convex combination of measurements. Indeed, one can perform a convex combination of measurements by a probabilistic mixture of each measurement. Therefore, the corresponding measurement of a convex combination of E and E' should also be performed by the probabilistic mixture of F and F' (the corresponding measurements of E and E') with the same weight. Finally, the correspondent of the trivial measurement (u) (i.e., 1-valued measurement) should be again the trivial measurement (u). From these considerations (in particular for yes-no measurements), we can give the formal definition of state-equivalence as follows:

Definition 1 (*Physical Equivalence of States*) *We say that state s_1 is physically equivalent to state s_2 if there exists a unit-preserving affine bijection $\Phi : \mathcal{E} \rightarrow \mathcal{E}$ such that $e(s_1) = \Phi(e)(s_2)$ for any $e \in \mathcal{E}$.*

We denote by $s_1 \simeq s_2$ iff s_1 is physically equivalent to s_2 . It is easy to see that \simeq is an equivalence relation: (i) $s \simeq s$, (ii) $s_1 \simeq s_2 \Rightarrow s_2 \simeq s_1$ and (iii) $s_1 \simeq s_2, s_2 \simeq s_3 \Rightarrow s_1 \simeq s_3$ for any $s, s_1, s_2, s_3 \in \mathcal{S}$. (Use identity map on \mathcal{E} , an inverse map and composition of maps on \mathcal{E} as the above map Φ):

Proposition 1 *Physical equivalence \simeq is an equivalence relation.*

Based on this operationally motivated definition, we consider the following principle:

[P5] (Physical Equivalence of Pure States) *Any pure states s_1 and s_2 are physically equivalent.*

The following result gives an equivalent characterization of the physical equivalence in terms of the structure of state space:

Theorem 2 *States s_1 and s_2 are physically equivalent iff there exists an affine bijection $\Psi : \mathcal{S} \rightarrow \mathcal{S}$ such that $s_1 = \Psi(s_2)$.*

To prove this theorem, we start from the following fact on effects: The set of effect $\mathcal{E} = \mathcal{E}(\mathcal{S})$ has a natural order relation defined by

$$e \geq f \Leftrightarrow e(s) \geq f(s) \quad \forall s \in \mathcal{S}$$

for effects $e, f \in \mathcal{E}$. Note that u and 0 are maximum and minimum effects.

Lemma 1 *Let $\Phi : \mathcal{E} \rightarrow \mathcal{E}$ be an affine bijection. Then the following three conditions are equivalent:*

1. $\Phi(0) = 0$
2. If $e, f \in \mathcal{E}$ and $e \leq f$, then $\Phi(e) \leq \Phi(f)$
3. $\Phi(u) = u$

(The proof is given in Appendix D. This lemma is used just for justifying that we have assumed in Definition 1 only the latter one of the two conditions $\Phi(0) = 0$ and $\Phi(u) = u$.)

Now we introduce the dual maps of affine bijections on \mathcal{E} and \mathcal{S} , respectively.

First, let $\Phi : \mathcal{E} \rightarrow \mathcal{E}$ be an affine bijection on \mathcal{E} such that $\Phi(u) = u$ (and thus $\Phi(0) = 0$ from Lemma 1). Then, the dual map $\Phi^* : \mathcal{S} \rightarrow \mathcal{S}$ on \mathcal{S} is defined by

$$\Phi^*(s)(e) := s(\Phi(e)) \quad (\forall s \in \mathcal{S}, e \in \mathcal{E}). \quad (3)$$

(See Eq. (2) for the notation.) We notice that Eq. (3) for fixed $s \in \mathcal{S}$ defines an affine functional on \mathcal{E} satisfying conditions in Theorem 1. To see this, let $\Lambda := \Phi^*(s)$. For any $\lambda \in [0, 1], e_1, e_2 \in \mathcal{E}$, we have $\Lambda(\lambda e_1 + (1 - \lambda)e_2) = s(\Phi(\lambda e_1 + (1 - \lambda)e_2)) = s(\lambda \Phi(e_1) + (1 - \lambda)\Phi(e_2)) = \lambda s(\Phi(e_1)) + (1 - \lambda)s(\Phi(e_2)) = \lambda \Lambda(e_1) + (1 - \lambda)\Lambda(e_2)$, and thus Λ is an affine functional on \mathcal{E} . Since $s(e) \in [0, 1]$ for any $e \in \mathcal{E}$, the range of Λ is in $[0, 1]$. Finally, $\Lambda(u) = s(\Phi(u)) = s(u) = 1$ and $\Lambda(0) = s(\Phi(0)) = s(0) = 0$. Thus Φ^* is a well-defined map on \mathcal{S} from Theorem 1.

Notice that, for any $\lambda \in [0, 1], s_1, s_2 \in \mathcal{S}$, one has $\Phi^*(\lambda s_1 + (1 - \lambda)s_2)(e) = (\lambda s_1 + (1 - \lambda)s_2)(\Phi(e)) =$

$(\lambda\Phi^*(s_1) + (1-\lambda)\Phi^*(s_2))(e) \ (\forall e \in \mathcal{E})$, hence Φ^* is affine on \mathcal{S} . Let $\Phi^*(s_1) = \Phi^*(s_2)$ for some states $s_1, s_2 \in \mathcal{S}$. Then, since $f := \Phi^{-1}(e) \in \mathcal{E}$ for any $e \in \mathcal{E}$, we have $s_1(e) = s_1(\Phi(\Phi^{-1}(e))) = \Phi^*(s_1)(f) = \Phi^*(s_2)(f) = s_2(\Phi(\Phi^{-1}(e))) = s_2(e)$. Therefore, from the separation hypothesis for states, we have $s_1 = s_2$, i.e., Φ^* is injective (one-to-one). Notice that Φ^{-1} is also an affine bijection on \mathcal{E} such that $\Phi^{-1}(u) = u$ and $\Phi^{-1}(0) = 0$. For an arbitrary $s \in \mathcal{S}$, define $t := (\Phi^{-1})^*(s) \in \mathcal{S}$, and it follows that for any $e \in \mathcal{E}$

$$\Phi^*(t)(e) = t(\Phi(e)) = s(\Phi^{-1}(\Phi(e))) = s(e),$$

and again from the separation hypothesis for states, we have $s = \Phi^*(t)$. Therefore, Φ^* is surjective, hence an affine bijection on \mathcal{S} .

On the other hand, the dual map of the affine bijection $\Psi : \mathcal{S} \rightarrow \mathcal{S}$ is easily defined by

$$\Psi^*(e)(s) := e(\Psi(s)) \ (\forall e \in \mathcal{E}, s \in \mathcal{S}). \quad (4)$$

Since the above defined $\Psi^*(e)$ is obviously an affine functional on \mathcal{S} to $[0, 1]$, $\Psi^*(e)$ is an effect. It is easy to see that Ψ^* is bijective on \mathcal{E} and satisfies $\Psi^*(u) = u$ (and $\Psi^*(0) = 0$).

Finally, it is also easy to see that both dual maps on \mathcal{E} and \mathcal{S} satisfy $(\Phi^*)^* = \Phi$ and $(\Psi^*)^* = \Psi$ from the definitions. To sum up, we have obtained

Proposition 2 (i) For any affine bijection $\Phi : \mathcal{E} \rightarrow \mathcal{E}$ such that $\Phi(u) = u$ (and thus $\Phi(0) = 0$), the dual map $\Phi^* : \mathcal{S} \rightarrow \mathcal{S}$ is well-defined by Eq. (3) and is affine bijective. (ii) For any affine bijection $\Psi : \mathcal{S} \rightarrow \mathcal{S}$, the dual map Ψ^* is well-defined by Eq. (4) and is affine bijective satisfying $\Psi^*(u) = u$ (and thus $\Psi^*(0) = 0$). (iii) For both bijections, $(\Phi^*)^* = \Phi$ and $(\Psi^*)^* = \Psi$.

Now we can give the proof of Theorem 2:

[Proof of Theorem 2] Let s_1, s_2 be physically equivalent, i.e., there exists a bijective affine $\Phi : \mathcal{E} \rightarrow \mathcal{E}$ such that $e(s_1) = \Phi(e)(s_2)$ for any $e \in \mathcal{E}$ and $\Phi(u) = u$ (and thus $\Phi(0) = 0$ from Lemma 1). From Proposition 2 (i), $\Psi := \Phi^*$ gives an affine bijection on \mathcal{S} . From Eq. (3), we have $\Psi(s_2)(e) = s_2(\Phi(e)) = \Phi(e)(s_2) = e(s_1) = s_1(e)$ for any $e \in \mathcal{E}$, and thus $s_1 = \Psi(s_2)$.

Conversely, assume that there exists an affine bijection $\Psi : \mathcal{S} \rightarrow \mathcal{S}$ such that $s_1 = \Psi(s_2)$. Then, from Proposition 2 (ii), the dual map $\Phi := \Psi^*$ is an affine bijection on \mathcal{E} satisfying that $\Phi(e)(s_2) = \Psi^*(e)(s_2) = e(\Psi(s_2)) = e(s_1)$ and $\Phi(u) = u$. Therefore, states s_1, s_2 are physically equivalent. ■

From Theorem 2, [P5] is equivalently rephrased as follows:

[P5'] For any given pure states $s_1, s_2 \in \mathcal{S}$, there exists a bijective affine map Ψ on \mathcal{S} such that $s_2 = \Psi(s_1)$.

In [19], we introduced the principle of equality of pure states intuitively meaning [P5] but have used [P5'] as its formal definition. Theorem 2 establishes its operational meaning as an equivalence of pure states. Some authors

[8–10] also have used [P5'] meaning that there are reversible transformations (dynamics) which connects any pure states. Thus, we have shown the equivalence of two superficially different physical principles.

On the other hand, from the mathematical and physical interests, Davies [26] have investigated the following condition:

[P5''] The group of affine bijections on \mathcal{S} acts transitively on the set of extreme points of \mathcal{S} .

It turns out that [P5], [P5'], and [P5''] are all equivalent: To see this, let $\mathcal{A}_b(\mathcal{S}, \mathcal{S})$ be the set of affine bijections on \mathcal{S} . One can show that $\mathcal{A}_b(\mathcal{S}, \mathcal{S})$ forms a compact group which acts continuously on \mathcal{S} [26]. Note that an affine bijection on \mathcal{S} maps a pure state to a pure state [41]. Therefore, it is straightforward that [P5'] holds iff affine bijections on \mathcal{S} acts transitively on $\mathcal{S}_{\text{pure}}$, i.e., $\mathcal{S}_{\text{pure}} = \{\Psi(s) \mid \Psi \in \mathcal{A}_b(\mathcal{S}, \mathcal{S})\}$ with arbitrary reference pure state $s \in \mathcal{S}_{\text{pure}}$.

In the following, we prefer to interpret the above equivalent conditions as a physical equivalence among any pure states [P5]. Indeed, as is the case for any basic physical theories so far, a symmetry is one of the key factor to understand our world, and [P5] enables us to interpret, without appealing to dynamics, that there exists an operationally motivated symmetry in the set of pure states. Of course, this is a matter of taste, and the following argument follows for those who prefer [P5'] or [P5'']. However, following Davies, we call GPTs satisfying [P5] (or equivalently [P5'] or [P5'']) *symmetric GPTs*.

1. Examples of Symmetric GPTs

Both classical theory and QM are symmetric GPTs. Indeed, for any pure states $\mathbf{p}^{(\mu)}, \mathbf{p}^{(\nu)} \in \mathcal{S}_{cl}$ with some $\mu, \nu = 1, \dots, d$, let Ψ be a map on \mathcal{S}_{cl} defined by $[\Psi(\mathbf{p})]_\mu = p_\nu, [\Psi(\mathbf{p})]_\nu = p_\mu$ and $[\Psi(\mathbf{p})]_i = p_i$ ($i \neq \mu, \nu$). Obviously Ψ is an affine bijection on \mathcal{S}_{cl} satisfying $\Psi(\mathbf{p}^\mu) = \mathbf{p}^\nu$. In quantum system, for any pure states $\rho_1 := |\psi_1\rangle\langle\psi_1|, \rho_2 := |\psi_2\rangle\langle\psi_2| \in \mathcal{S}_q$, one can easily find a unitary operator $U : \mathcal{H}_d \rightarrow \mathcal{H}_d$ such that $U\psi_2 = \psi_1$ [42]. Then it is easy to see that $\Psi(\rho) := U\rho U^\dagger$ is an affine bijection on \mathcal{S}_q satisfying $\rho_1 = \Psi(\rho_2)$.

Another simple example of symmetric GPTs are cuboid systems [27]:

[Example 3] (Cuboid Systems) We call GPTs cuboid systems if the state spaces are represented by hypercubes: $\mathcal{S}_{cube} := \{\mathbf{x} \in \mathbb{R}^d \mid 0 \leq x_i \leq 1 \ (i = 1, \dots, d)\}$. There are 2^d pure states (vertices): $\mathbf{x}^{(i_1, i_2, \dots, i_d)} := (i_1, i_2, \dots, i_d)$ ($i_1, \dots, i_d = 0, 1$).

It is easy to see that the cuboid system \mathcal{S}_{cube} is also symmetric. In general, any isogonal figure is symmetric from the definition:

[Example 4] (Systems with Isogonal Figures) A polytope in Euclidean space is said to be isogonal iff for any vertices there exists an isometrical map which surjectively connects them [28]. (Notice that any isometrical map on Euclidean space is automatically affine.) Therefore, any

GPTs with state space being isogonal figure are symmetric.

2. Invariant States

In this section, we discuss an invariant state (the maximal mixed state) in GPTs.

In general GPTs, the existence of an invariant state with respect to all the bijective affine maps on \mathcal{S} can be shown based on Ryll-Rardzewski fixed point theorem.

Theorem 3 *For any GPT, there exists an invariant state $s_{inv} \in \mathcal{S}$ with respect to all the bijective affine maps on \mathcal{S} .*

[Proof] We refer to [29, 30] for Ryll-Rardzewski fixed point theorem. Using the norm in Appendix B, the underlying vector space V of \mathcal{S} is a Banach space w.r.t. the sup-norm and \mathcal{S} is a compact convex subset of V . Since we assumed $\dim V < \infty$, all topologies in the Ryll-Rardzewski theorem are equivalent to the norm topology. Let $G = A_b(\mathcal{S}, \mathcal{S})$ be the set of all the bijective affine maps on \mathcal{S} . Then, it is easy to show that G is a semigroup of (weakly) continuous affine maps of \mathcal{S} . In particular, G is noncontractive on \mathcal{S} , since the norm $\|\cdot\|$ satisfies $\inf_{\Phi \in G} \|\Phi(s_1) - \Phi(s_2)\| = \|s_1 - s_2\| > 0$ ($\forall s_1 \neq s_2 \in \mathcal{S}$) from Lemma 4 in Appendix B. Applying the Ryll-Rardzewski theorem, the assertion of the theorem holds. ■

In general GPT, an invariant state is not necessarily unique. (For instance, consider a GPT with the state space being a circular sector $\mathcal{S} = \{(r \cos \theta, r \sin \theta) | 0 \leq r \leq 1, 0 \leq \theta \leq \frac{\pi}{2}\}$. Then, there are only two affine bijections on \mathcal{S} : the identity map and the reflection map with respect to the 45 degree axis. Then, all the states on the axis are invariant under these maps.) However, in a symmetric GPT, the unique invariant state is determined.

Theorem 4 *In a symmetric GPT, an invariant state is unique.*

[Proof] Assume that there exist distinct invariant states s_1, s_2 on \mathcal{S} . Then, any state of the form $ps_1 + (1-p)s_2 \in \mathcal{S}$ for any $p \in \mathbb{R}$ is invariant under any bijective affine $\Psi : \mathcal{S} \rightarrow \mathcal{S}$ (See Lemma 5 in Appendix C). In particular, there exists such state s_3 on a boundary of \mathcal{S} . Let $H \subset V$ be the supporting hyperplane of \mathcal{S} on s_3 and let $s_3 = \sum_{i=0}^n p_i t_i$ ($p_i > 0$) ($n \in \mathbb{N}$) be a convex decomposition of s_3 with respect to pure states $\{t_i\}$. Then, since $s_3 \in H$ and H is a supporting hyperplane of \mathcal{S} , we have $t_i \in H \cap \mathcal{S}$ for every t_i . Notice that there exists a pure state $s_0 \in \mathcal{S}$ not in H . (Otherwise, $\mathcal{S} \subset H$.) Since \mathcal{S} is symmetric, there exists an affine bijective map Ψ which connects t_0 and s_0 : $s_0 = f(t_0)$. However, we have $\sum_{i=0}^n p_i t_i = s_3 = f(s_3) = \sum_{i=0}^n p_i f(t_i) = p_0 s_0 + p_1 f(t_1) \cdots$, and this is contradictory. ■

In the following, s_M denotes an invariant state, which is uniquely determined for symmetric GPTs. For a GPT

with polytope state space, where the set of pure states is $\{s_1, \dots, s_n\}$, we have

$$s_M = \frac{1}{n} \sum_{i=1}^n s_i. \quad (5)$$

Indeed, as any bijective affine Φ on \mathcal{S} maps any pure state to a pure state, Φ just permutes finite numbers of pure states, and we have $\Phi(s_M) = \frac{1}{n} \sum_{i=1}^n \Phi(s_i) = s_M$. In particular, in classical system, s_M is the uniform distribution on Ω : $s_M = (1/d, \dots, 1/d)$. For cuboid systems, we have $s_M = (1/2, 1/2, \dots, 1/2)$, i.e., the center of \mathcal{S}_{cube} .

In the case of finite quantum systems, notice that bijective affine map on \mathcal{S}_q is unitary map or anti-unitary map on the density operators [31]. Therefore, the maximally mixed state

$$s_M = \frac{1}{d} \mathbb{I}$$

is the unique invariant state.

In general, the construction [26] of s_M is given by the two-sided Haar measure [32]: Using the two-sided Haar measure on the set G of all the affine bijection on \mathcal{S} , we have

$$s_M = \int_G \Psi(s_0) d\mu(\Psi), \quad (6)$$

where $s_0 \in \mathcal{S}$ is an arbitrary reference state (See also [33] for the mathematical details). Indeed, the unique existence of the invariant states of Symmetric GPTs is first shown by Davies [26] by means of the Haar measure.

Note that an operationally natural entropy in general GPTs is defined by

$$S(s) := \inf_{M=(m_j)_j \in M_{ind}} H(m_j(s)), \quad (7)$$

where $H(p_j) := -\sum_j p_j \log_2 p_j$ is the Shannon entropy and the infimum is taken over the set M_{ind} of all the indecomposable measurements [19, 34]. S is concave on \mathcal{S} , generalizing Shannon and von Neumann entropies in classical and quantum systems, respectively. In a symmetric GPT, S takes minimum value 0 on pure states, and thus S provides a proper measure of mixedness [19]. Therefore, the following proposition implies that we may call s_M the maximal mixed state in general (symmetric) GPT.

Proposition 3 *In any GPT, the entropy S takes the maximal value on an invariant state.*

[Proof] Notice that for a bijective affine Ψ on \mathcal{S} and indecomposable measurement $M = (m_j)_j$, $(m_j \circ \Psi)_j$ is an indecomposable measurement [19]. Thus, we have $S(\Psi(s)) = S(s)$ for any state s . Then, from the concavity of S , for any state s , the invariant state s_M obtained by (6) from the reference state $s_0 := s$ satisfies

$$S(s_M) \geq \int_G S(\Psi(s)) d\mu(\Psi) = \int_G S(s) d\mu(\Psi) = S(s).$$

The next result shows a global picture of a state space \mathcal{S} in symmetric GPT. Let D be a distance function which have the monotonicity properties under affine bijection on \mathcal{S} , i.e., for any states $s_1, s_2 \in \mathcal{S}$ and any affine bijection $\Psi : \mathcal{S} \rightarrow \mathcal{S}$, $D(s_1, s_2) \geq D(\Psi(s_1), \Psi(s_2))$. The typical example is given by the Kolmogorov distance (See Appendix B).

Proposition 4 *In symmetric GPTs, for any distance function D on \mathcal{S} with the monotonicity property, the distances between s_M and arbitrary pure states are constant. Namely, for any pure states s_1, s_2 ,*

$$D(s_1, s_M) = D(s_2, s_M) \quad (8)$$

[Proof] From the symmetry of \mathcal{S} , there exists an affine bijection Ψ on \mathcal{S} such that $s_1 = \Psi(s_2)$. From the monotonicity of D and the invariance of s_M , we have

$$D(s_1, s_M) = D(\Psi(s_2), \Psi(s_M)) \leq D(s_2, s_M).$$

The opposite inequality follows by a symmetric argument. \blacksquare

Geometrically speaking, all the pure states of symmetric GPTs lie on the sphere with respect to the distance with the monotonicity property, e.g. Kolmogorov distance. In the case of Kolmogorov distance (B2), physical meaning of (8) is that the optimal success probability to distinguish between the invariant state s_M and any pure state s is constant on s (See Eq. (B2) in Appendix B).

3. Classification of Symmetric GPTs

Now we proceed to the classification theorem of Symmetric GPTs. First, remind that without loss of generality, \mathcal{S} is a compact subset of \mathbb{R}^d , and by the parallel shift, we can assume the invariant state s_M of G to be the origin of \mathbb{R}^d .

Using the Haar measure on the set of G of all the affine bijection on \mathcal{S} , one can define a G -invariant inner product by $\langle x, y \rangle_G := \int_G \langle \Psi x, \Psi y \rangle d\mu(\Psi)$ where the right-hand side is the Haar integral and $\langle x, y \rangle$ denotes the Euclidean inner product of $x, y \in \mathbb{R}^d$. Then, using an orthonormal basis w.r.t. this G -invariant basis, we get to a new state-representation in \mathbb{R}^d such that $\Psi \in G$ acts isometrically on states. Remind that, in Sec. III A 1 (Example 4), we have just illustrated symmetric GPTs with state spaces being isogonal figures, but now it earns the general symmetric GPTs if the numbers of pure states are finite:

Proposition 5 *The state space \mathcal{S} of a symmetric GPT is either one of isogonal figures or with infinite pure states.*

In [33], we further obtain the following classification theorems of symmetric GPTs in 2 and 3 dimensional cases:

Theorem 5 *The state space \mathcal{S} of symmetric GPTs with $\dim(\text{Aff } \mathcal{S}) = 2$ is either an isogonal figure or a unit disk.*

Theorem 6 *The state space \mathcal{S} of symmetric GPTs with $\dim(\text{Aff } \mathcal{S}) = 3$ is any one of an isogonal figure, a circular cylinder, or a unit disk (ball).*

B. Decomposability of states with distinguishable pure states

In this section, we consider another principle of the decomposability of states with respect to distinguishable pure states.

Remind that states $\{s_1, \dots, s_n\}$ are said to be distinguishable if they can be distinguishable with probability 1 in a single shot measurement; namely if there exists a measurement $M = (e_i)_{i=1}^n$ such that $e_i(s_j) = \delta_{ij}$ for any $i, j = 1, \dots, n$. The maximum number of distinguishable states is an important parameter to characterize GPTs, and is denoted as c . In classical systems, c is the number (cardinality) of the sample space Ω_c , while in quantum systems it is the dimension of the corresponding Hilbert space \mathcal{H}_c . In general GPT, c has the following upper bound:

Proposition 6 *In GPT with state space \mathcal{S} , we have*

$$c \leq \dim(\mathcal{S}) + 1. \quad (9)$$

The equality holds iff \mathcal{S} is a simplex.

To see this, observe the following lemma:

Lemma 2 *A distinguishable set of states $\{s_1, \dots, s_n\}$ is affinely independent. Therefore, $\text{Conv}\{s_i\}$ is an $(n - 1)$ dimensional simplex.*

[Proof] Let $\sum_{i=1}^n p_i s_i = \sum_{i=1}^n q_i s_i$ be convex combinations of $\{s_i\}_i$ w.r.t. probability distributions $(p_i)_i$ and $(q_i)_i$. Then, applying a measurement $M = (e_i)_i$ which distinguishes $\{s_i\}_i$, we get $p_i = q_i$, and thus $\{s_i\}_i$ is affinely independent (See [39]). \blacksquare

[Proof of Proposition 6] Let $\{s_1, \dots, s_c\}$ be a set of distinguishable states. Then, from Lemma 2, $\text{Conv}\{s_i\}$ is a $(c - 1)$ dimensional simplex. As $\text{Conv}\{s_i\} \subset \mathcal{S}$, we have $c - 1 \leq \dim(\mathcal{S})$.

Let the equality of Eq. (9) holds. Let $d := \dim(\mathcal{S})$ and let $\{s_1, \dots, s_{d+1}\}$ be distinguishable states with a measurement $M = (m_j)_{j=1}^{d+1}$ which distinguishes them. Note that, from Lemma 2, $\text{Conv}\{s_i\}_{i=1}^{d+1}$ is a d -dimensional simplex. We show that $\mathcal{S} = \text{Conv}\{s_i\}_{i=1}^{d+1}$. To see this, notice that the dimension of $\text{Aff}\{s_i\}_{i=1}^{d+1}$ is d and $\{s_i\}_{i=1}^{d+1} \subset \mathcal{S}$, and thus $\text{Aff}\{s_i\}_{i=1}^{d+1} = \text{Aff } \mathcal{S}$. Therefore, any $s \in \mathcal{S}$ can be written as $s = \sum_{i=1}^{d+1} \lambda_i s_i$ with some $\lambda_i \in \mathbb{R}$ satisfying $\sum_i \lambda_i = 1$. Applying m_i to s (See Lemma 5 in Appendix C), we obtain $\lambda_i = m_i(s) \geq 0$, and thus $s \in \text{Conv}\{s_i\}_{i=1}^{d+1}$. Therefore, we have $\mathcal{S} \subset \text{Conv}\{s_i\}_{i=1}^{d+1}$. As $s_i \in \mathcal{S}$, we obtain $\mathcal{S} = \text{Conv}\{s_i\}_{i=1}^{d+1}$. Namely, \mathcal{S} is d dimensional simplex. \blacksquare

In both classical and quantum systems, any state is written as a convex combination of distinguishable pure states. (Note that any classical state $\mathbf{p} = (p_1, \dots, p_d)$ has the decomposition $\mathbf{p} = \sum_{\mu=1}^d p_{\mu} \mathbf{p}^{\mu}$, while any quantum state ρ has a decomposition $\rho = \sum_{i=1}^c p_i |\psi_i\rangle\langle\psi_i|$ as an eigenvalue decomposition of ρ .) This property can be physically phrased as following physical principle:

[P6] (Decomposability with Distinguishable Pure States) *Any state can be prepared as a probabilistic mixture of distinguishable pure states.*

It is interesting to consider GPTs satisfying this principle, which include both classical and quantum systems. We notice that this property is derived from their axioms in [11].

The following result provides the general classification of such GPTs:

Theorem 7 *GPTs satisfying [P6] is either classical system or systems with infinite pure states.*

To prove this, we use the following lemma:

Lemma 3 *If \mathcal{S} is a d dimensional polytope satisfying the principle [P6], then there exist $d+1$ distinguishable states.*

[Proof] The case $d = 0$ is trivial. Let $d \geq 1$. Let \mathcal{F} be the family of all subsets of \mathcal{S} such that it is the convex hull of at most d pure states of \mathcal{S} . Since \mathcal{S} is a polytope, the number of pure states is finite, therefore the size of \mathcal{F} is also finite. Now each subset of \mathcal{S} in \mathcal{F} is at most $(d-1)$ -dimensional, therefore its d -dimensional volume is 0. Hence the union $\bigcup \mathcal{F}$ of all (finitely many) members of \mathcal{F} also has d -dimensional volume 0, while \mathcal{S} has positive d -dimensional volume. This implies that \mathcal{S} contains a state s that does not belong to $\bigcup \mathcal{F}$. By the principle of [P6], s is a convex combination of distinguishable pure states s_1, \dots, s_k , and now $k > d$ by the definition of \mathcal{F} and s . Hence the claim holds. ■

[Proof of Theorem 7] Let the number of pure states be finite, i.e., \mathcal{S} be a polytope. From Lemma 3, there exist $d+1$ distinguishable states. Therefore, the equality of Eq. (9) holds and thus from Proposition 6, \mathcal{S} is simplex, i.e., a state space with a classical system. ■

C. Classification of GPTs with [P5] and [P6]

Combining the classifications of GPTs with [P5] and [P6], i.e., Theorem 5, Theorem 6 for [P5] and Theorem 7 for [P6], we obtain the following:

Theorem 8 *The state space \mathcal{S} of GPTs satisfying [P5] and [P6] with $\dim \mathcal{S} = 2, 3$ is either simplex or unit disk.*

This result implies that GPTs with principles [P5] and [P6] such that the state space is embedded in 2 or 3 dimensional real vector space is restricted to either classical system or quantum system (qubit).

Notice that this does not hold in higher dimensional GPTs as quantum systems with more than or equal to 3 level systems satisfy both [P5] and [P6] while the state space is neither the simplex nor the ball [35].

IV. CONCLUSION AND DISCUSSION

In this paper, after confirming our basis of general GPTs (namely, Principles [P1]-[P4]), we have introduced and investigated two physical principles [P5] (Physical Equivalence of Pure States) and [P6] (Decomposability with Distinguishable Pure States). In particular, the former is established with the operationally motivated definition of physical equivalence of states, which turns out to be equivalent to the symmetric structure of the state space (See Sec. III A). In each principle, we gave a classification of state spaces (Theorems 5, 6 for [P5] and 7) for [P6]) and by combining them, we showed that GPTs with 2 or 3 dimensional state spaces are either classical or quantum system (with the Bloch ball) (Theorem 8). Note that similar characterizations of the Bloch ball are derived in [8–11]. However, the definition of the Bloch ball there is the state space of systems with at most two distinguishable states, while our derivation does not assume the maximum number of distinguishable states. In this paper, we focused on simple principles on states and measurements, and showed how each principle narrows down GPTs close to classical and quantum systems. In near future, we further consider other principles on especially correlations on composite systems, and discuss the characterization of QM by purely physical principles.

Acknowledgment

We are grateful to Dr. Miyadera and Dr. Imafuku for their useful discussion. One of the authors (G.K.) would like to thank Prof. D’Ariano, Dr. Chiribella, and Dr. Perinotti for their fruitful discussion and comments at Nagoya Winter Workshop, 18-24 February (2010). This work was partially supported by Grant-in-Aid for Young Scientists (B) (No.20700017 and No.22740079), The Ministry of Education, Culture, Sports, Science and Technology (MEXT), Japan.

Appendix A

In this appendix, we give a proof of Representation 1 which is formally described by the following Theorem:

Theorem 9 *Assume [P1]-[P3] and let \mathcal{S} be the state space. Then, there exist a real vector space V and a representation map $\hat{\cdot} : \mathcal{S} \rightarrow V$ such that (i) the map $\hat{\cdot}$ is injective (one-to-one) and $\widehat{\langle p; s_1, s_2 \rangle} = p\hat{s}_1 + (1-p)\hat{s}_2$; (thus $\hat{\mathcal{S}}$ is a convex subset of V and pure states correspond to extreme points of $\hat{\mathcal{S}}$), and (ii) an n -valued measurement M is represented by an n -tuple of effects $(e_i)_{i=1}^n$ on $\hat{\mathcal{S}}$ such that $\Pr\{M = i|s\} = e_i(\hat{s})$ for any $s \in \mathcal{S}$ (and thus $\sum_i e_i = u$ where u is the unit effect).*

[Proof] We call a real functional $f : \mathcal{S} \rightarrow \mathbb{R}$ an “affine” functional iff $f(\langle p; s_1, s_2 \rangle) = pf(s_1) + (1-p)f(s_2)$ for any $s_1, s_2 \in \mathcal{S}$ and $p \in [0, 1]$. Also an “affine” functional e on \mathcal{S} is called an “effect” if the range is in $[0, 1]$. The unit

“effect” u is the effect such that $u(s) = 1$ for any $s \in \mathcal{S}$. We denote by $\mathcal{A}(\mathcal{S})$ and $\mathcal{E}(\mathcal{S})$ the set of all the “affine” functionals and “effects” on \mathcal{S} . It is easy to see that $\mathcal{A}(\mathcal{S})$ forms a real vector space with pointwise addition and scalar multiplication, while $\mathcal{E}(\mathcal{S})$ is a convex subset of $\mathcal{A}(\mathcal{S})$.

Let M be an n -valued measurement. Then, the probability $\Pr\{M = i|s\}$ with a fixed i is considered as a map from \mathcal{S} to $[0, 1]$:

$$s \in \mathcal{S} \rightarrow e_i(s) := \Pr\{M = i|s\} \quad (i = 1, \dots, n), \quad (\text{A1})$$

which are clearly “effects” from [P3-1]. Remind that measurements are characterized only through probabilities from [P2-2]. Thus M is characterized by n -tuple of “effects” $(e_i)_{i=1}^n$ where $e_i \in \mathcal{E}(\mathcal{S})$ is defined by (A1). From the normalization condition of the probability, we have $\sum_{i=1}^n e_i = u$. In the following, we denote by $M = (e_i)_{i=1}^n$ an n -valued measurement meaning that $e_i(s)$ is the probability to get i th outcome when performing M under state s . Note that the part (ii) of Theorem 9 is an easy consequence of this representation of measurements. (See the last part of this proof.)

Next, let V be the set of all the affine functionals on $\mathcal{E}(\mathcal{S})$ with bounded ranges. It is easy to see that V is a real vector space with pointwise addition and scalar multiplication. Now we define a state-representation map $\hat{\cdot}: \mathcal{S} \rightarrow V$ by

$$\hat{s}(e) := e(s) \quad (\forall e \in \mathcal{E}(\mathcal{S})). \quad (\text{A2})$$

Note that \hat{s} is an affine functional on $\mathcal{E}(\mathcal{S})$ by the definition, while the range of \hat{s} is bounded since $0 \leq e(s) \leq 1$, thus $\hat{\cdot}$ maps any state to a vector in V . Let $\hat{s}_1 = \hat{s}_2$ for $s_1, s_2 \in \mathcal{S}$. Then $e(s_1) = \hat{s}_1(e) = \hat{s}_2(e) = e(s_2)$ for any “effect” e . Therefore, for any measurement $M = (e_i)_{i=1}^n$, $\Pr\{M = m_i|s_1\} = e_i(s_1) = e_i(s_2) = \Pr\{M = m_i|s_2\}$, which implies $s_1 = s_2$ from [P2-1]. Thus, $\hat{\cdot}$ is injective. From the “affinity of effect”, $\langle p; \hat{s}_1, \hat{s}_2 \rangle(e) = e(\langle p; s_1, s_2 \rangle) = pe(s_1) + (1-p)e(s_2) = (p\hat{s}_1 + (1-p)\hat{s}_2)(e)$ for any $e \in \mathcal{E}(\mathcal{S})$. Thus, the state $s = \langle p; s_1, s_2 \rangle$ is mapped to be a convex combination of \hat{s}_1 and \hat{s}_2 :

$$\langle p; \hat{s}_1, \hat{s}_2 \rangle = p\hat{s}_1 + (1-p)\hat{s}_2. \quad (\text{A3})$$

Notice that from [P3-1] the set $\hat{\mathcal{S}} := \{\hat{s} \in V | s \in \mathcal{S}\}$, which is the state-space of this representation, is a convex subset of V . It is straightforward from the definition that pure states are mapped to extreme points of $\hat{\mathcal{S}}$, and vice versa. This completes the proof of part (i) of Theorem 9.

Finally, let $\tilde{\cdot}$ be a representation map on $\mathcal{E}(\mathcal{S})$ to the set of affine functionals on $\hat{\mathcal{S}}$ defined by $\tilde{e}(\hat{s}) := e(s) \quad (\forall s \in \mathcal{S})$. It is easy to see the injectivity and the affinity of $\tilde{\cdot}$. Since the range of \tilde{e} for $e \in \mathcal{E}$ is in $[0, 1]$, \tilde{e} is an effect on $\hat{\mathcal{S}}$. Therefore, any n -valued measurement M is represented by an n -tuple of effects $(\tilde{e}_i)_{i=1}^n$ on $\hat{\mathcal{S}}$ such that $\sum_i \tilde{e}_i$ is the unit effect and $\Pr\{M = i|s\} = \tilde{e}_i(\hat{s})$ for any $s \in \mathcal{S}$. ■

The representation symbols $\hat{\cdot}$ and $\tilde{\cdot}$ are all omitted throughout this paper except in the above proof.

Appendix B: “Physical Topology” on State Space

In this appendix, we review a physical topology and show Representation 2 in finite dimensional cases. For the readers’ convenience and mathematical simplicity, we explain these using a Kolmogorov distance.

Remind from Appendix A that each vector in V is a bounded affine functional on $\mathcal{E}(\mathcal{S})$. Then, one can introduce a natural norm on V by

$$\|v\| := \sup_{e \in \mathcal{E}} |v(e)|. \quad (\text{B1})$$

(Notice that $\|v\| < \infty$ as v is a bounded functional on \mathcal{E} ; it is clear that (i) $\|v\| \geq 0$; (ii) $\|v\| = 0$ iff $v = 0$; (iii) $\|\alpha v\| = |\alpha|\|v\|$; (iv) $\|v + w\| \leq \|v\| + \|w\|$ for all $v, w \in V$ and $\alpha \in \mathbb{R}$.) Notice that the norm of any state s is 1 as $|e(s)| \leq 1$ for all $e \in \mathcal{E}$ and $u(s) = 1$. Thus, \mathcal{S} lies on the unit sphere with respect to this norm. The induced metric

$$D_{kol}(v, w) := \|v - w\| \quad (v, w \in V)$$

is called the Kolmogorov distance [36], since it is a straightforward generalization of the Kolmogorov distance in classical systems. In QM, the norm and distance are the trace norm and trace distance. The Kolmogorov distance on \mathcal{S} has an operational meaning through the relation

$$D_{kol}(s_1, s_2) = 2P(s_1, s_2) - 1, \quad (\text{B2})$$

where $P(s_1, s_2)$ is the optimal success probability to distinguish states s_1 and s_2 which are prepared with probabilities $1/2$ and $1/2$ (see [19] and references therein). Therefore, the topology with respect to this norm has an operational meaning as states s_1 and s_2 are close w.r.t. this norm iff the optimal success probability to distinguish them are close to $1/2$.

From (B2), state space \mathcal{S} is bounded in V with this norm as probabilities are in $[0, 1]$. In general, \mathcal{S} might not be closed. However, with a physical consideration, it turns out that without loss of generality one can assume \mathcal{S} is closed. Indeed, even if there exists an “imaginary state” $v \in V$ in the closure of \mathcal{S} which is not in \mathcal{S} , there exists a state $s \in \mathcal{S}$ arbitrary close to v with this norm. Namely, for any small $\varepsilon > 0$, there exists a state s such that $|v(e) - s(e)| < \varepsilon$ for any $e \in \mathcal{E}$. Thus, under the presence of an (arbitrary small but) finite error as always the cases in the real experiments, it is impossible to (even statistically) distinguish the “imaginary state” and state s through all the possible measurements. Therefore, it is a matter of taste to include or not every “imaginary states” as states.

To sum up, one can assume that \mathcal{S} is represented as a closed and bounded convex subset of a normed space V . Note that, if $\dim V < \infty$, compactness and closed boundedness are equivalent from the Heine-Borel Theorem for general normed space [37]. Moreover, in that case, this topology is the same as the physical topology

[13] due to the uniqueness of the topology of the locally convex Hausdorff topological vector space.

We note the monotonicity holds [19] for any affine map Ψ on \mathcal{S} :

$$\|\Psi(s)\| \leq \|s\|. \quad (\text{B3})$$

and thus

$$\|\Psi(s_1) - \Psi(s_2)\| \leq \|s_1 - s_2\| \quad (\forall s_1, s_2 \in \mathcal{S}). \quad (\text{B4})$$

Applying this for an affine bijection on \mathcal{S} , we get the following:

Lemma 4 *Any affine bijection Ψ on \mathcal{S} preserves the Kolmogorov distance:*

$$\|\Psi(s_1) - \Psi(s_2)\| = \|s_1 - s_2\|.$$

Proof Apply (B4) for Ψ and Ψ^{-1} . \blacksquare

Appendix C: Extension of affine maps

Let V_1, V_2 be real vector spaces and W be a convex subset of V_1 . Then, any affine map $\Lambda : W \rightarrow V_2$ has an affine extension to V_1 . With some additional conditions, Λ is further extended to a linear map on V_1 .

In this appendix, we present the proof of these facts for finite dimensional cases [43]: Let $\dim V_1 < \infty$. Throughout this section, Λ is an affine map from W to V_2 .

Lemma 5 *Let $w_i \in W$ and $\lambda_i \in \mathbb{R}$ ($i = 1, \dots, m$) with $\sum_i \lambda_i = 1$. If $\sum_{i=1}^m \lambda_i w_i \in W$, then*

$$\Lambda\left(\sum_{i=1}^m \lambda_i w_i\right) = \sum_{i=1}^m \lambda_i \Lambda(w_i). \quad (\text{C1})$$

Proof. Let $C_+ := \{i = \{1, \dots, m\} | \lambda_i \geq 0\}$ and $C_- := \{i = \{1, \dots, m\} | \lambda_i < 0\}$. Since $\sum_{i=1}^m \lambda_i = 1$, it follows that $1 + \sum_{i \in C_-} |\lambda_i| = \sum_{i \in C_+} |\lambda_i|$, and thus $C_+ \neq \emptyset$, $\sum_{i \in C_+} |\lambda_i| =: \lambda \geq 1$, $|\lambda_i| \leq \lambda$ for any $i = 1, \dots, m$. Letting $w := \sum_{i=1}^m \lambda_i w_i \in W$, we have

$$\frac{1}{\lambda} w + \sum_{i \in C_-} \frac{|\lambda_i|}{\lambda} w_i = \sum_{i \in C_+} \frac{|\lambda_i|}{\lambda} w_i,$$

where both right and left sides are convex combinations of vectors from W . From the affinity of Λ , we have

$$\frac{1}{\lambda} \Lambda(w) + \sum_{i \in C_-} \frac{|\lambda_i|}{\lambda} \Lambda(w_i) = \sum_{i \in C_+} \frac{|\lambda_i|}{\lambda} \Lambda(w_i),$$

which implies (C1). \blacksquare

Proposition 7 *Λ has an affine extension $\tilde{\Lambda}$ to V_1 with the form*

$$\tilde{\Lambda}(v) = Av + b \quad (\text{C2})$$

where A is a linear map from V_1 to V_2 and $b \in V_2$. If $\text{Aff}(W) = V_1$, then the extension is unique.

Proof. Let $\dim \text{Aff}(W) = n$ and $\dim V_1 = n + m$ ($m \geq 0$). Let $w_i \in W$ ($i = 0, \dots, n$) be affinely independent set so that $w_i - w_0$ ($i = 1, \dots, n$) are linearly independent. Let $\{v_i\}_{i=1}^{n+m}$ be a basis of V_1 such that $v_i = w_i - w_0$ for $i = 1, \dots, n$. Then, define a map $\tilde{\Lambda} : V_1 \rightarrow V_2$ in (C2) with a linear map $A : V_1 \rightarrow V_2$ and $b \in V_2$ given by

$$Av_i := \begin{cases} \Lambda(w_i) - \Lambda(w_0) & i = 1, \dots, n \\ v'_i & i = n + 1, \dots, n + m \end{cases}$$

$$b := \Lambda(w_0) - Aw_0$$

where v'_i are arbitrary vectors in V_2 . Then, one can show that $\tilde{\Lambda}$ is an affine extension of Λ . To see this, note first that any $w \in W$ is uniquely written by $w = \sum_{i=0}^n \lambda_i w_i$ with $\lambda_i \in \mathbb{R}$ such that $\sum_{i=0}^n \lambda_i = 1$ since $\{w_i\}_{i=0}^n$ are affinely independent and n is the dimension of W . Then, for any $w = \sum_{i=0}^n \lambda_i w_i \in W$, it follows that $\tilde{\Lambda}(w) = (\sum_{i=1}^n \lambda_i Aw_i) + \lambda_0 Aw_0 + (\Lambda(w_0) - Aw_0) = \sum_{i=1}^n \lambda_i (Aw_0 + \Lambda(w_i) - \Lambda(w_0)) + \lambda_0 Aw_0 + (\Lambda(w_0) - Aw_0) = \sum_{i=0}^n \lambda_i \Lambda(w_i) - \lambda_0 \Lambda(w_0) + (1 - \lambda_0)(Aw_0 - \Lambda(w_0)) + \lambda_0 Aw_0 + (\Lambda(w_0) - Aw_0) = \Lambda(w)$, where we have used Lemma 5 in the final equation. Affinity of $\tilde{\Lambda}$ follows from the form of (C2).

Let $\text{Aff}(W) = V_1$. Assume that $\tilde{\Lambda}$ and $\tilde{\Lambda}'$ are affine extensions of Λ . Noting that any vector $v \in V_1 = \text{Aff}(W)$ is uniquely written by $v = \sum_{i=0}^n \lambda_i w_i$ with $\sum_{i=0}^n \lambda_i = 1$, we have $\tilde{\Lambda}(v) = \sum_{i=0}^n \lambda_i \tilde{\Lambda}(w_i) = \sum_{i=0}^n \lambda_i \Lambda(w_i) = \sum_{i=0}^n \lambda_i \tilde{\Lambda}'(w_i) = \tilde{\Lambda}'(v)$ by the same argument as Lemma 5 (note that each w_i is in the domain W of Λ). Thus the uniqueness of the extension follows. \blacksquare

The following result gives a linear extension of Λ :

Proposition 8 (i) *If $0 \notin \text{Aff}(W)$, Λ has always a linear extension to V_1 . In particular, if $\dim V_1 = \dim \text{Aff}(W) + 1$, the extension is unique.* (ii) *If $0 \in \text{Aff}(W)$, then Λ does not necessarily have linear extensions. In particular, in the case $0 \in W$, Λ has a linear extension to V_1 iff $\Lambda(0) = 0$.*

Proof. Here we use the same notation as in the proof of Proposition 7.

(i) Let $0 \notin \text{Aff}(W)$. Obviously, $\text{Aff}(W) \neq V_1$ and $m \geq 1$. Using the basis $\{v_i\}_{i=1}^{n+m}$, let $-w_0 = \sum_{i=1}^{n+m} x_i v_i$ with some $x_i \in \mathbb{R}$. Then, there exists at least one non-zero coefficient x_i ($i = n + 1, \dots, m$); Otherwise we have $-w_0 = \sum_{i=1}^n x_i (w_i - w_0)$ and thus $0 = \sum_{i=1}^n x_i w_i + (1 - \sum_{i=1}^n x_i) w_0 \in \text{Aff}(W)$, which contradicts $0 \notin \text{Aff}(W)$. Without loss of generality, let $x_{n+1} \neq 0$ and choose $v'_{n+1} = -\frac{1}{x_{n+1}}(\Lambda(w_0) + \sum_{i=1}^n x_i (\Lambda(w_i) - \Lambda(w_0)))$ and $v'_i = 0$ ($i = n + 2, \dots, n + m$). Then, a direct computation shows that $Aw_0 = \Lambda(w_0)$, i.e., $b = 0$.

Next, we show the uniqueness of the linear extension for the case $\dim V = \dim \text{Aff}(W) + 1$, i.e., $m = 1$. In this case, one can choose $v_{n+1} := w_0$ in a basis $\{v_i\}_{i=1}^{n+1}$. Indeed, if $\sum_{i=1}^n \alpha_i (w_i - w_0) + \alpha_{n+1} w_0 = 0$ and at least one α_i is non-zero, then $\alpha_{n+1} \neq 0$ by linear independence of $w_i - w_0 = v_i$ ($1 \leq i \leq n$), but this implies $0 \in \text{Aff}(W)$, which is a contradiction. Therefore, $\{v_i\}_{i=1}^n$ with $v_i =$

$w_i - w_0$ and $v_{n+1} = w_0$ is an independent system of V and thus gives its basis. Let A and A' give linear extensions of Λ . Then, using the above basis, any vector $v \in V$ is written as $v = \sum_i x_i(w_i - w_0) + x_{n+1}w_0$. Since $Aw = \Lambda(w) = A'w$ for any $w \in W$, we have $Av = A'v$ for any $v \in V$. This proves the uniqueness of the extension.

(ii) Let $0 \in W$. Then $b = \Lambda(0)$. Therefore, in this case, an affine map can be linearly extended iff $\Lambda(0) = 0$. ■

It is well-known that a quantum operation Λ on the set \mathcal{S}_q of density operators is uniquely extended to a linear map on a vector space $\mathcal{L}(\mathcal{H}_d)$ of all the linear operators on a Hilbert space \mathcal{H}_d . While there are several ways to show this extension, it can be derived from Proposition 8 as an easy corollary. Indeed, it is easy to check that \mathcal{S}_q is a convex subset of a real vector space $V_1 := \mathcal{L}(\mathcal{H})_h$ of the set of Hermitian operators, satisfying $0 \notin \text{Aff}(\mathcal{S}_q)$ and $\dim \mathcal{L}(\mathcal{H})_h = \dim \text{Aff}(\mathcal{S}_q) + 1$. Therefore, one can uniquely extend Λ to a linear map $\tilde{\Lambda}$ on $\mathcal{L}(\mathcal{H})_h$. Next, noting that any linear operator $A \in \mathcal{L}(\mathcal{H})$ is uniquely decomposed into the sum of real and imaginary parts, i.e., $A = A_R + iA_I$ where $A_R := \frac{1}{2}(A + A^\dagger)$ and $A_I := \frac{1}{2i}(A - A^\dagger)$, one can further extend $\tilde{\Lambda}$ to a linear map $\tilde{\tilde{\Lambda}}$ on $\mathcal{L}(\mathcal{H})$ by $\tilde{\tilde{\Lambda}}(A) := \tilde{\Lambda}(A_R) + i\tilde{\Lambda}(A_I)$.

We notice that, in general GPTs, one can also treat operations (including dynamical map and measurement processes) described by its linear extension in a similar manner.

In the following, we assume $\text{Aff}(W) = V_1 = V_2$ and let $\Lambda : W \rightarrow W$ be an affine map on W . We show that any surjective affine map on W is affinely extended to a bijective map on $V := V_1$.

Lemma 6 *If Λ is surjective on W , so is the affine extension $\tilde{\Lambda} : V \rightarrow V$ on V .*

Proof As $\text{Aff}(W) = V$, an arbitrary $y \in V$ is written as $y = \sum_{i=0}^n \lambda_i w_i$ with some $\lambda_i \in \mathbb{R}$ and $\sum_i \lambda_i = 1$. From the surjectivity of Λ on W , there exists w'_i such that $w_i = \Lambda(w'_i)$ ($\forall i = 0, \dots, n$). Therefore, we have $y = \sum_i \lambda_i \Lambda(w'_i) = \sum_i \lambda_i (Aw'_i + b) = A(\sum_i \lambda_i w'_i) + b = \tilde{\Lambda}(\sum_i \lambda_i w'_i)$. Thus, $\tilde{\Lambda}$ is surjective on V . ■

Proposition 9 *If Λ is surjective on W , then $\tilde{\Lambda} : V \rightarrow V$ and Λ are bijective.*

Proof From the previous Lemma, $\tilde{\Lambda}$ is surjective on V and so is the linear map $A : V \rightarrow V$ which composes Λ . Remind that a linear map on a finite dimensional vector space is surjective iff it is injective. Therefore, A is bijective and so is $\tilde{\Lambda}$ on V . Injectivity of Λ on W follows since it is a restriction of the injective map $\tilde{\Lambda}$ to W . ■

Appendix D

In this appendix, we give proofs of Lemma 1 and Theorem 1.

[Proof of Lemma 1] ($1 \Rightarrow 2$) If $e \leq f$, then $g := f/2$ and $k := f - e$ are clearly effects. As $g = (f + 0)/2 = (e + k)/2 \in \mathcal{E}$, we have $\Phi(g) = (\Phi(f) + \Phi(0))/2 = (\Phi(e) + \Phi(k))/2$. Since $\Phi(0) = 0$, we have $\Phi(f) = \Phi(e) + \Phi(k)$, and thus $\Phi(e) \leq \Phi(f)$. ($2 \Rightarrow 3$) By the relation $\Phi^{-1}(u) \leq u$ and the assumption, we have $u = \Phi(\Phi^{-1}(u)) \leq \Phi(u)$, therefore $\Phi(u) = u$. ($3 \Rightarrow 1$) For any $g \in \mathcal{E}$, $u - g \in \mathcal{E}$ and thus $(\Phi(g) + \Phi(u - g))/2 = (\Phi(u) + \Phi(0))/2 \in \mathcal{E}$. Since $\Phi(u) = u$, we get $\Phi(g) + \Phi(u - g) - \Phi(0) = u \geq \Phi(u - g)$, therefore $\Phi(g) \geq \Phi(0)$. Put $g = \Phi^{-1}(0)$, we have $0 \geq \Phi(0)$, and thus $0 = \Phi(0)$. ■

Let $\mathcal{S} \subset \mathbb{R}^d$ with $\text{Aff}(\mathcal{S}) = \mathbb{R}^d$, then from Proposition 7, any effect $e \in \mathcal{E}$ is uniquely represented by $a \in \mathbb{R}^d, b \in \mathbb{R}$ such that

$$e(s) = \langle a, s \rangle + b,$$

where $\langle \cdot, \cdot \rangle$ represents the Euclidean inner product in \mathbb{R}^n . (Remind that any real linear functional $A : \mathbb{R}^d \rightarrow \mathbb{R}$ is uniquely represented by a vector $a \in \mathbb{R}^n$ such that $Ax = \langle a, x \rangle$ for any $x \in \mathbb{R}^d$.) Let a map $\tilde{\cdot} : \mathcal{E} \rightarrow \mathbb{R}^{d+1}$ be defined by $\tilde{e} = (a, b)$, then it is easy to see that $\tilde{\cdot}$ is an affine injection and \mathcal{E} is a convex subset in \mathbb{R}^{d+1} . In particular, $\tilde{u} = (0, 1)$ and $\tilde{0} = (0, 0)$.

[Proof of Theorem 1] Let $\tilde{\Lambda}$ be an affine functional on $\tilde{\mathcal{E}}$ defined by $\tilde{\Lambda}(\tilde{e}) := \Lambda(e)$. Note that $(0, 0) = \tilde{0} \in \tilde{\mathcal{E}}$ and $\tilde{\Lambda}(0, 0) = \Lambda(0) = 0$. Thus, from Proposition 8, $\tilde{\Lambda}$ can be represented by a vector $(x, y) \in \mathbb{R}^d \times \mathbb{R} = \mathbb{R}^{d+1}$ such that

$$\tilde{\Lambda}(a, b) = \langle (x, y), (a, b) \rangle = \langle x, a \rangle + yb.$$

Since $1 = \Lambda(u) = \tilde{\Lambda}(0, 1)$, we have $y = 1$:

$$\tilde{\Lambda}(a, b) = \langle x, a \rangle + b.$$

In the following, we prove that $s := x \in \mathcal{S}$, and thus for any effect $e \in \mathcal{E}$ with $\tilde{e} = (a, b)$, we have $\Lambda(e) = \tilde{\Lambda}(a, b) = \langle s, a \rangle + b = e(s)$.

To prove this, assume contrary that $x \notin \mathcal{S}$, then there exists a hyperplane which strictly separates $\{x\}$ and \mathcal{S} (see Theorem 4.12 in [23]); Equivalently, there exists a (continuous) affine functional $f : \mathbb{R}^d \rightarrow \mathbb{R}$ such that $f(x) < 0$ and $f(t) > 0$ for any $t \in \mathcal{S}$. Then, $f' := \frac{1}{\max_{t \in \mathcal{S}} f(t)} f$ is an effect such that $0 > f'(x)$. Note that f' can be represented as $f'(z) = \langle a_0, z \rangle + b_0$ ($z \in \mathbb{R}^d$), and thus $\tilde{f}' = (a_0, b_0)$ from the uniqueness of the representation of effects. Thus, we have

$$0 > f'(x) = \langle a_0, x \rangle + b_0 = \tilde{\Lambda}(a_0, b_0) = \Lambda(f').$$

This contradicts that $\Lambda(e) \geq 0$ for any $e \in \mathcal{E}$.

Finally, the uniqueness follows from the separation hypothesis for states [P2-1]. ■

-
- [1] J. von Neumann, *Mathematische Grundlagen der Quantenmechanik* (Springer, Berlin, 1932).
- [2] G. Birkhoff and J. von Neumann, *Ann. Math.* **37**, 823 (1936); A. M. Gleason, *J. Math. Mech.* **6**, 885 (1957); C. Piron, *Helv. Phys. Acta*, **37**, 439 (1964); S. Pulmannova, *Int. J. Theor. Phys.* **35**, 2309 (1996).
- [3] P. Jordan, *et al.*, *Ann. Math.* **35**, 29 (1934); I. E. Segal, *Ann. Math.* **48**, 930 (1947).
- [4] G. Ludwig, *Foundations of Quantum Mechanics I,II* (Springer, 1983).
- [5] C. A. Fuchs, quant-ph/0205039.
- [6] R. Clifton, *et al.*, *Found. Phys.* **33**, 1561 (2003).
- [7] G. M.D'Ariano, arXiv:0807.4383. To appear in "Philosophy of Quantum Information and Entanglement" (Cambridge University Press, Cambridge UK); G. Chiribella, G. M. D'Ariano, and P. Perinotti, *Phys. Rev. A* **81**, 062348 (2010).
- [8] L. Hardy, arXiv:quant-ph/0101012.
- [9] B. Dakić and C. Brukner, arXiv:0911.0695.
- [10] L. Masanes, arXiv:1004.1483.
- [11] G. Chiribella, G. M. D'Ariano, and P. Perinotti, arXiv:1011.6451.
- [12] G. Mackey, *Mathematical Foundations of Quantum Mechanics* (Dover, 1963).
- [13] H. Araki, *Einführung in die Axiomatische Quantenfeldtheorie, I, II* (Lecture note distributed by Swiss Federal Institute of Technology, 1962); *Mathematical Theory of Quantum Fields* (Oxford University Press, 1999).
- [14] S. P. Gudder, *Stochastic Method in Quantum Mechanics* (Dover, 1979).
- [15] M. Ozawa, *Rep. Math. Phys.* **18**, 11 (1980).
- [16] A. S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory* (North-Holland, Amsterdam, 1982).
- [17] H. Barnum, J. Barrett, M. Leifer, and A. Wilce, *Phys. Rev. Lett.* **99**, 240501 (2007); *ibid*, arXiv:0805.3553.
- [18] K. Nuida, G. Kimura, and T. Miyadera, *J. Math. Phys.* **51**, 093505 (2010).
- [19] G. Kimura, K. Nuida, and H. Imai, *Rep. Math. Phys.* **66**, 175 (2010); arXiv:0910.0994.
- [20] G. Kimura, *Phys. Lett. A*, **314**, 339 (2003); G. Kimura and A. Kossakowski, *Open Sys. Information Dyn.*, **12**, 207 (2005).
- [21] K. Kraus *States, Effects, and Operations: Fundamental Notions of Quantum Theory* (Lecture Notes in Physics vol 190) (Berlin, 1983).
- [22] H. H. Schaefer, *Topological Vector Spaces* (2nd edition, Springer, 1999); G. Köthe, *Topological Vector Spaces* (Springer-Verlag, 1979).
- [23] S. R. Lay, *Convex Sets and Their Applications* (Krieger Publishing Company, 1982).
- [24] B. Davies and J. T. Lewis, *Comm. Math. Phys.* **17**, 239 (1970); M. Ozawa, *J. Math. Phys.* **25**, 79 (1984).
- [25] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge) 2000.
- [26] E. B. Davies, *Quart. J. Math. Oxford Ser.* **25**, 323 (1974).
- [27] G. Kimura, T. Miyadera, and H. Imai, *Phys. Rev. A* **79**, 062306 (2009).
- [28] P. R. Cromwell, *Polyhedra* (Cambridge University Press, 1997), p. 369.
- [29] C. Ryll-Nardzewski, *Bull. Acad. Polon. Sci. Ser. Sci. Math. Astronom. Phys.* **10**, 271 (1962); *Proc. 5-th Berkeley Symp. Probab. Math. Stat.*, 2: 1, Univ. California Press, 55 (1967).
- [30] S. Stratila, L. Zsido, *Lectures on von Neumann algebra* (Abacus Press, 1979).
- [31] R. Kadison, *Ann. Math.* **54**, 325 (1951).
- [32] K. H. Hofmann, S. A. Morris, *The Structure of Compact Groups* (Walter de Gruyter, 1998).
- [33] G. Kimura and K. Nuida, arXiv:1012.5350.
- [34] A. J. Short, S. Wehner, *New J. Phys.* **12**, 033023 (2010). H. Barnum, et al., arXiv:0909.5075.
- [35] G. Kimura, *Phys. Lett. A* **314**, 339 (2003); G. Kimura, A. Kossakowski, *Open Sys. Information Dyn.* **12**, 207 (2005).
- [36] C. A. Fuchs, J. Graaf, *IEEE Trans. Info. Theory* 45(4): 1216 (1999).
- [37] J. L. Kelley, *General Topology* (Springer, 1955).
- [38] In general setting, one may assume that each measurement M has a measurable space (Ω, \mathcal{F}) where Ω is a sample space for measurement outcomes and \mathcal{F} is a σ algebra for measurement events, e.g., $\Omega = \mathbb{R}$, $\mathcal{F} = \mathcal{B}(\mathbb{R})$. Then, for each event $\Delta \in \mathcal{F}$ and state s , a probability $\Pr\{\Delta \in \mathcal{B}(\mathbb{R})|s\}$ to get an outcome in Δ is determined.
- [39] A subset W is called a c dimensional simplex if it is a convex hull of affinely independent set $\{w_i\}_{i=1}^{c+1}$. Remind that $\{v_i \in V\}_{i=1}^{m+1}$ is called an affinely independent set iff $\lambda_i \in \mathbb{R}$ with $\sum_{i=1}^{m+1} \lambda_i = 0$ and $\sum_{i=1}^{m+1} \lambda_i v_i = 0$ implies $\lambda_i = 0$ ($\forall i = 1, \dots, m+1$). It is an easy exercise to show that the followings are all equivalent: (i) $\{v_i\}_{i=1}^{m+1}$ is an affinely independent set; (ii) For any i_0 , $\{v_i - v_{i_0}\}_{i \neq i_0}$ is a linearly independent set; (iii) Convex decomposition w.r.t. $\{v_i\}_{i=1}^{m+1}$ is unique. (Namely, if $\sum_{i=1}^{m+1} p_i v_i = \sum_{i=1}^{m+1} q_i v_i$ with probability distributions $(p_i)_i$ and $(q_i)_i$, then $p_i = q_i$ ($\forall i = 1, \dots, m+1$)).
- [40] In QM, we usually admit, especially in finite systems, that any Hermitian operator (called an observable) and unitary operation correspond to feasible measurement and dynamics, respectively. Then, given any POVM $(E_i)_{i=1}^n$ in quantum system, there exists an ancilla system described by Hilbert space \mathcal{H}_n , an initial state σ on \mathcal{H}_n , and unitary operator U on $\mathcal{H}_{tot} := \mathcal{H}_d \otimes \mathcal{H}_n$, and a meter observable $M = \sum_i m_i P_i$ on \mathcal{H}_n such that $\text{tr}(E_i \rho) = \text{tr}_{tot}(U(\rho \otimes \sigma)U^\dagger \mathbb{I} \otimes P_i)$.
- [41] Let $\Psi : \mathcal{S} \rightarrow \mathcal{S}$ be an affine bijection and let $s \in \mathcal{S}$ be a pure state. Let $\Psi(s) = ps_1 + (1-p)s_2$ with some $t_1, t_2 \in \mathcal{S}$ and $p \in (0, 1)$. Applying Ψ^{-1} , we have $s = p\Psi^{-1}(s_1) + (1-p)\Psi^{-1}(s_2)$ and thus $s = \Psi^{-1}(s_1) = \Psi^{-1}(s_2)$, as s is a pure state. Therefore, we have $\Psi(s) = s_1 = s_2$, and $\Psi(s)$ is a pure state.
- [42] For instance, let $\{\phi_i\}_{i=1}^d$ and $\{\phi'_j\}_{j=1}^d$ be orthonormal bases of \mathcal{H}_d such that $\phi_1 = \psi_1$ and $\phi'_1 = \psi_2$. Then, use a unitary operator $U := \sum_{i=1}^d |\phi_i\rangle\langle\phi'_i|$.
- [43] For infinite dimensional cases, by noting the existence of a basis of V_1 (guaranteed by Zorn's lemma), essentially the same proofs are applied.